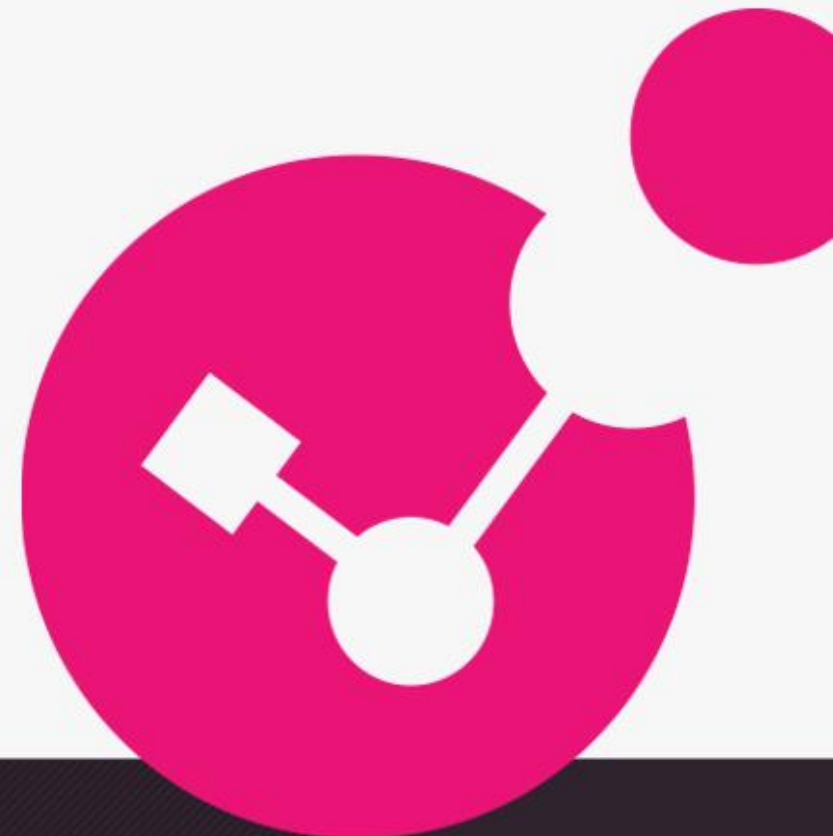




安全數位創新，防護敏捷轉型

全國大專校院資訊行政主管研討會

楊敦凱 Danny Yang, Cyber Security Evangelist
Check Point Software Technologies, Ltd.



YOU DESERVE THE BEST SECURITY

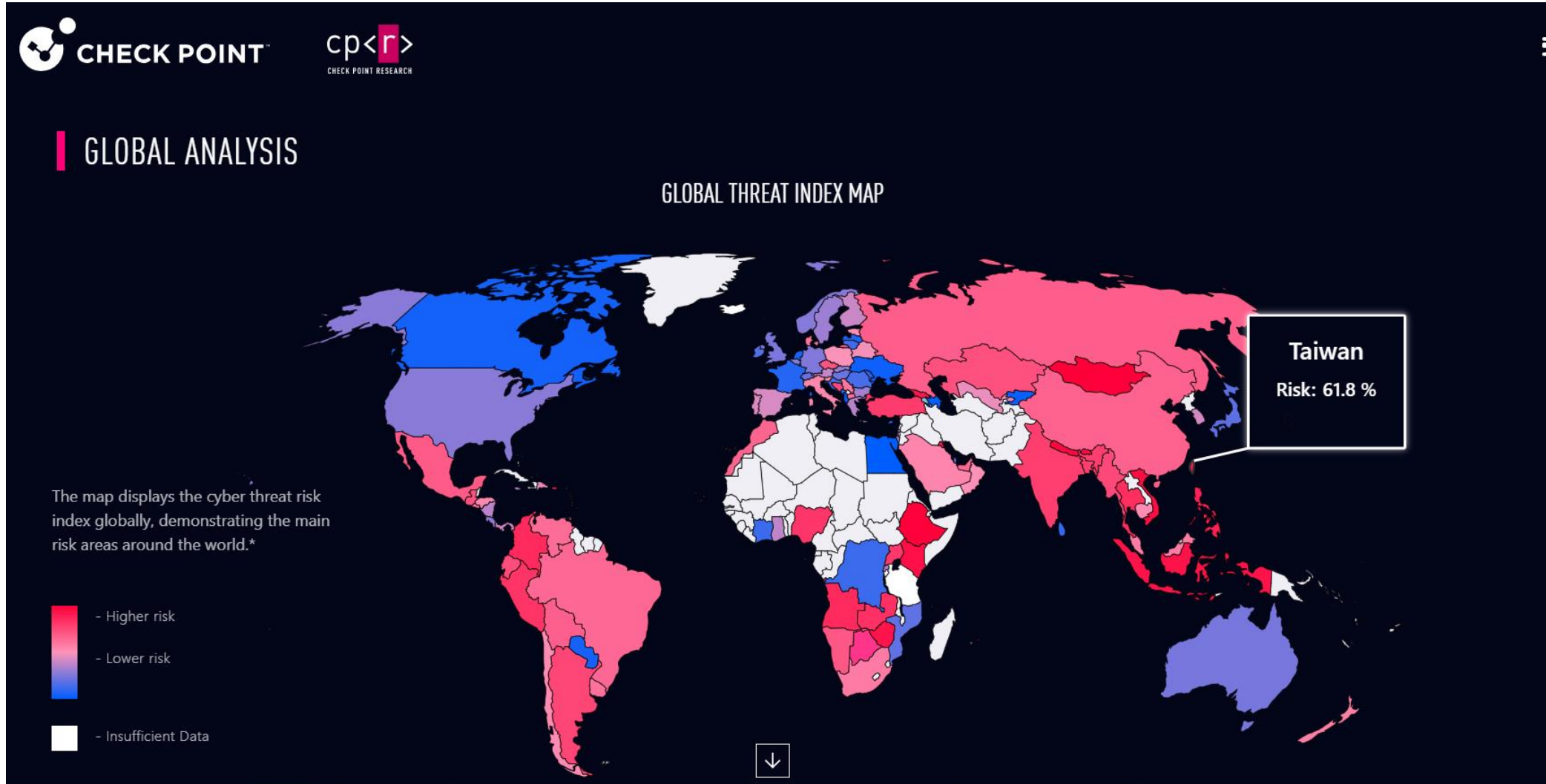


2023上半年安全威脅報告摘要

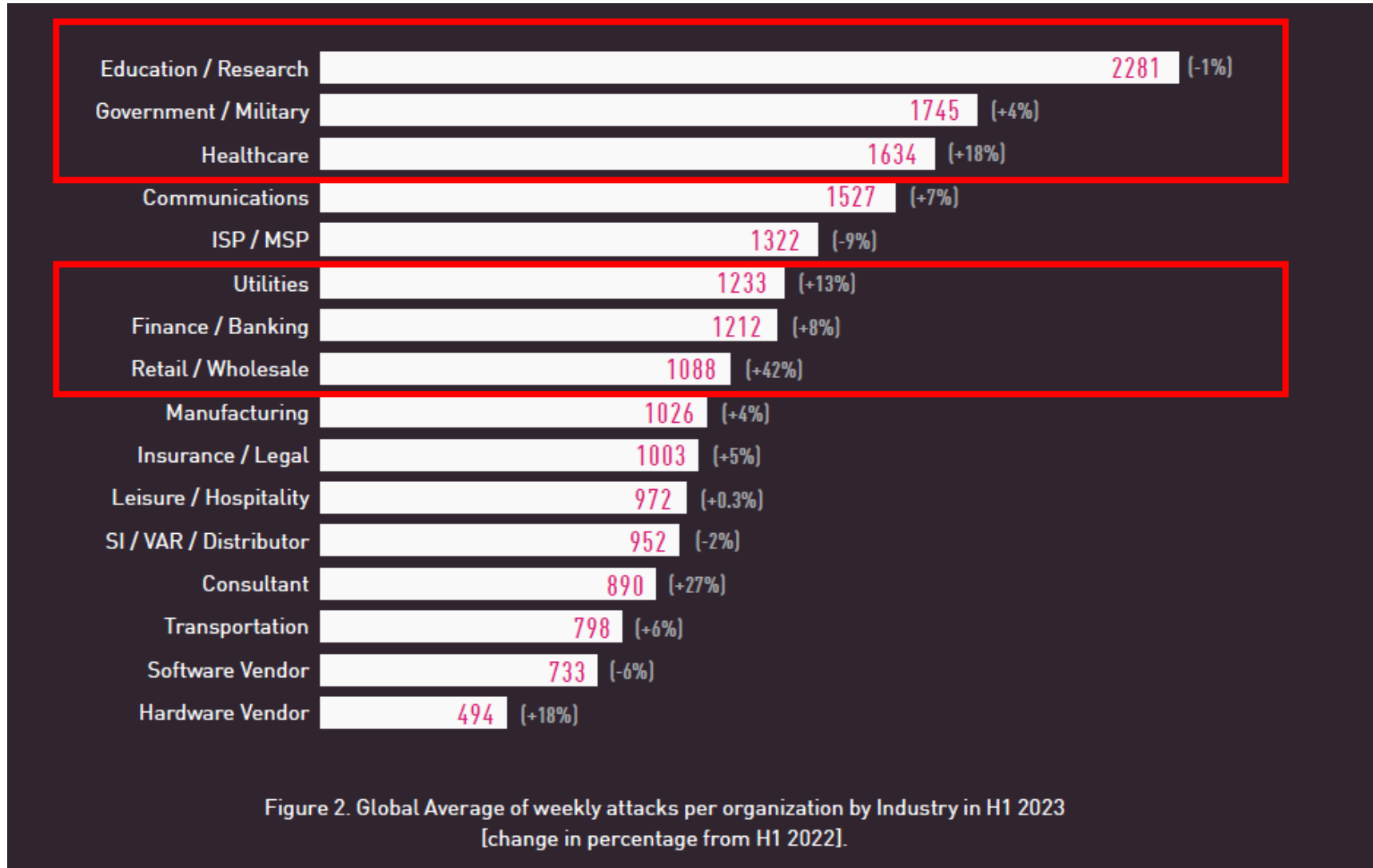
- **威脅分析:** 上半年網路犯罪活動持續升級，第二季全球每週攻擊激增8%，創下兩年來最高數量。(臺灣第一季遭攻擊數居全球之冠，每週達3,250次)
- **產業分析:** 排名前三的產業仍為教育與研究機構、政府、醫療
- **攻擊型態:** 透過郵件攻擊佔比達92%，以OneNote檔案的惡意威脅遽增(3,200%)
- **惡意程式分析:** 多重目的惡意程式(如Qbot, Emotet)與竊取資料類別(如Lokibot)在各地理區域仍極度猖獗，受勒索軟體影響最高的產業別為製造與零售業。
- **安全趨勢:** AI應用對資安產業的衝擊、勒索軟體組織發展、舊型態攻擊手段(USB)、激進駭客主義演進、日趨嚴重的行動威脅

2023 MID-YEAR
CYBER SECURITY
REPORT

臺灣位處全球攻擊熱區之一，風險係數超過60%



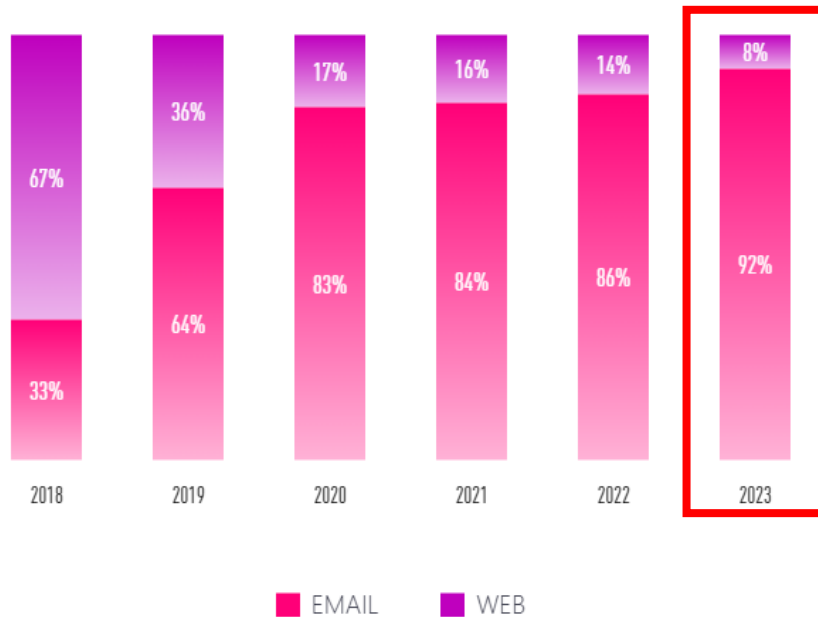
產業趨勢分析: 與2022年相比整體攻擊量仍持續增長



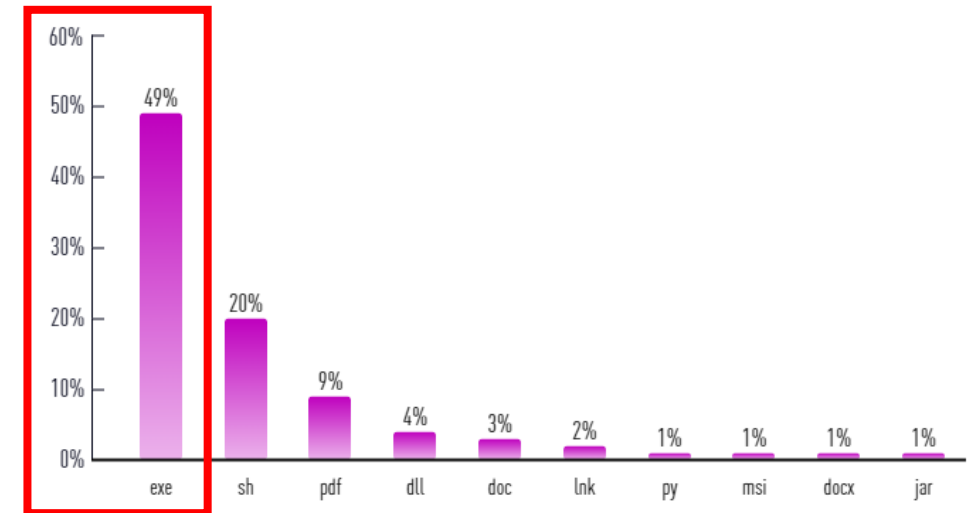
攻擊型態分析: 透由郵件而來的攻擊比例再創新高

TOP MALICIOUS FILE TYPES – WEB VS EMAIL

DELIVERY PROTOCOLS - EMAIL VS. WEB
ATTACK VECTORS IN 2018-2023.

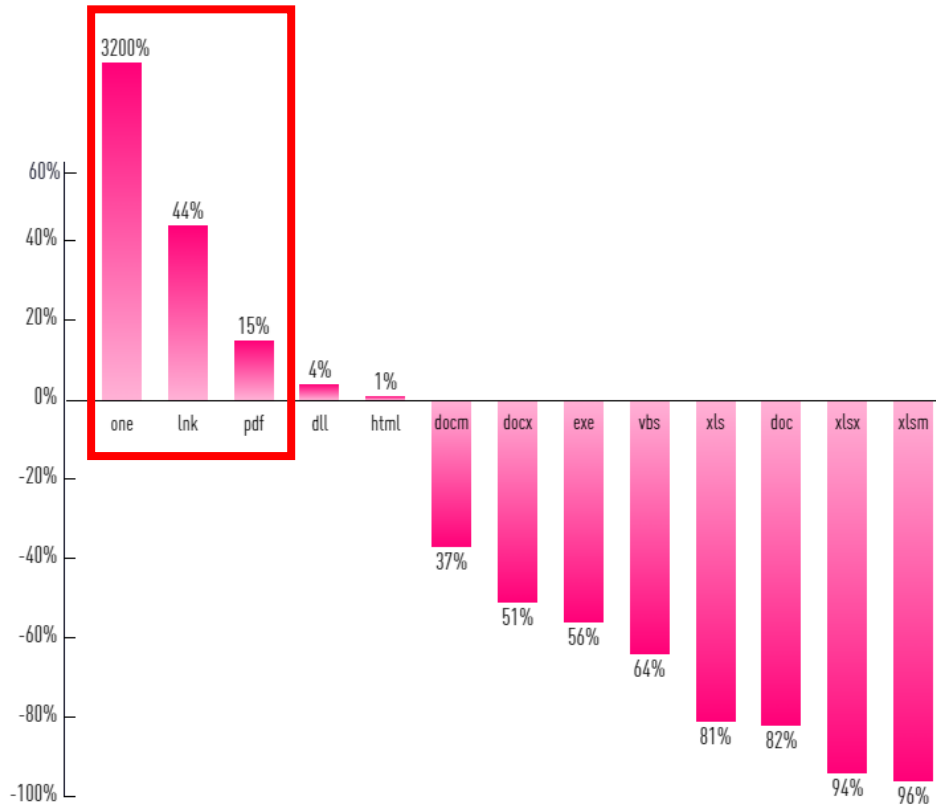


WEB DELIVERED MALICIOUS FILES
BY TYPE IN H1 2023.

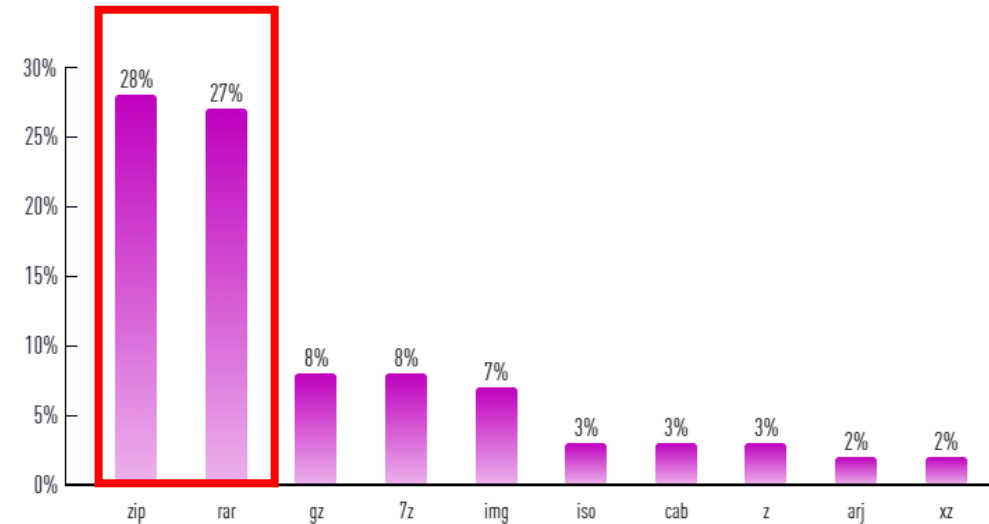


攻擊型態分析: 透由郵件而來的攻擊比例再創新高

EMAIL DELIVERED MALICIOUS FILES, CHANGE IN PREVALENCE IN H1 2023 COMPARED TO 2022.



EMAIL DELIVERED MALICIOUS ARCHIVE FILE TYPES IN H1 2023.



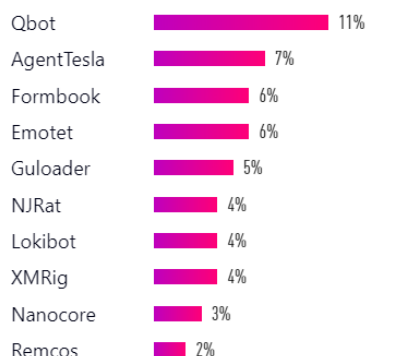
攻擊類型分析: 多重目的與竊取資訊惡意程式分布

Top惡意程式家族 (依地理區域)

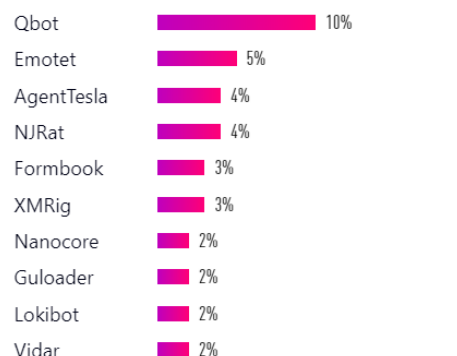
Top惡意網域 (TOP LEVEL DOMAIN)

TOP MALWARE FAMILIES

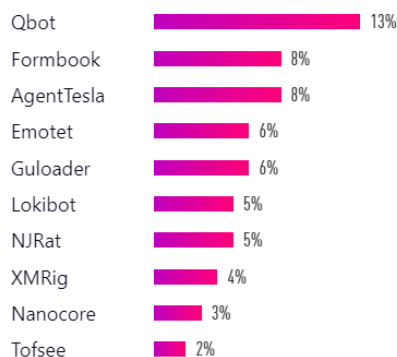
MOST PREVALENT MALWARE GLOBALLY



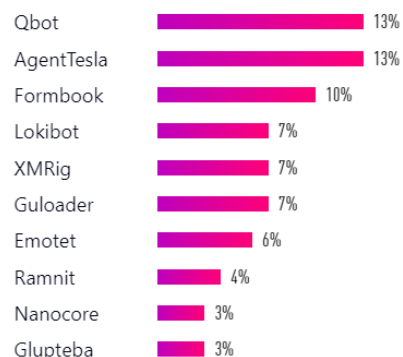
MOST PREVALENT MALWARE IN THE AMERIC/



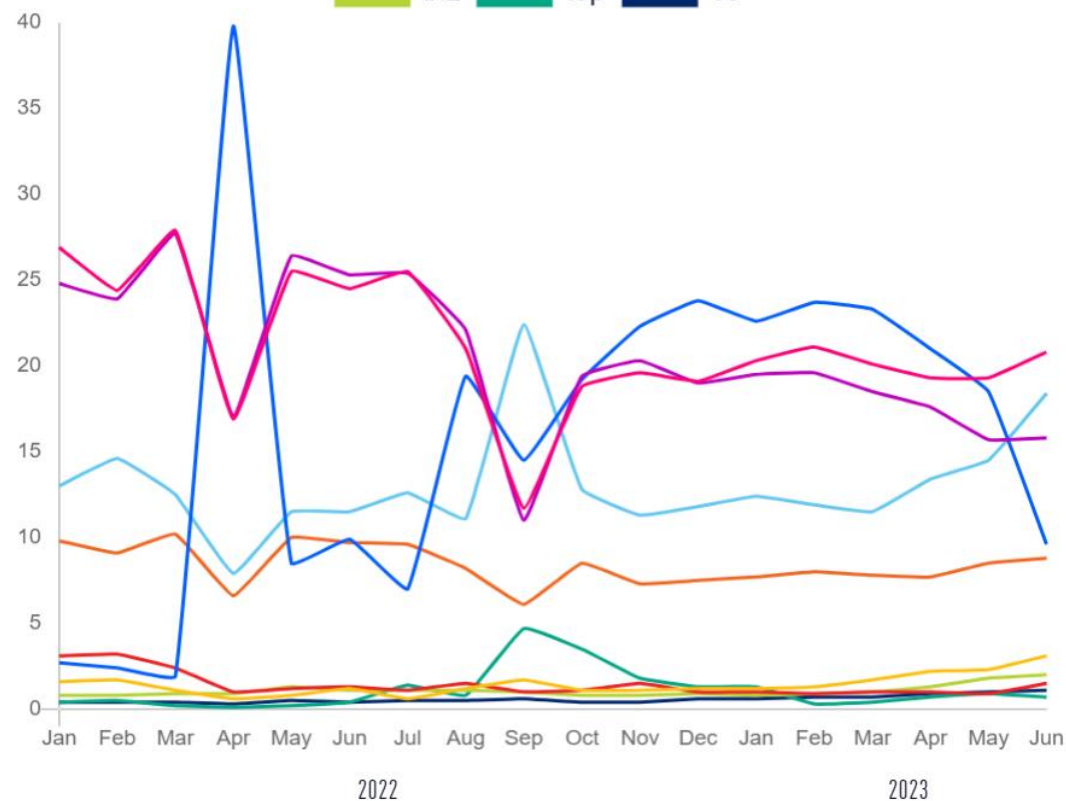
MOST PREVALENT MALWARE IN EMEA



MOST PREVALENT MALWARE IN APAC

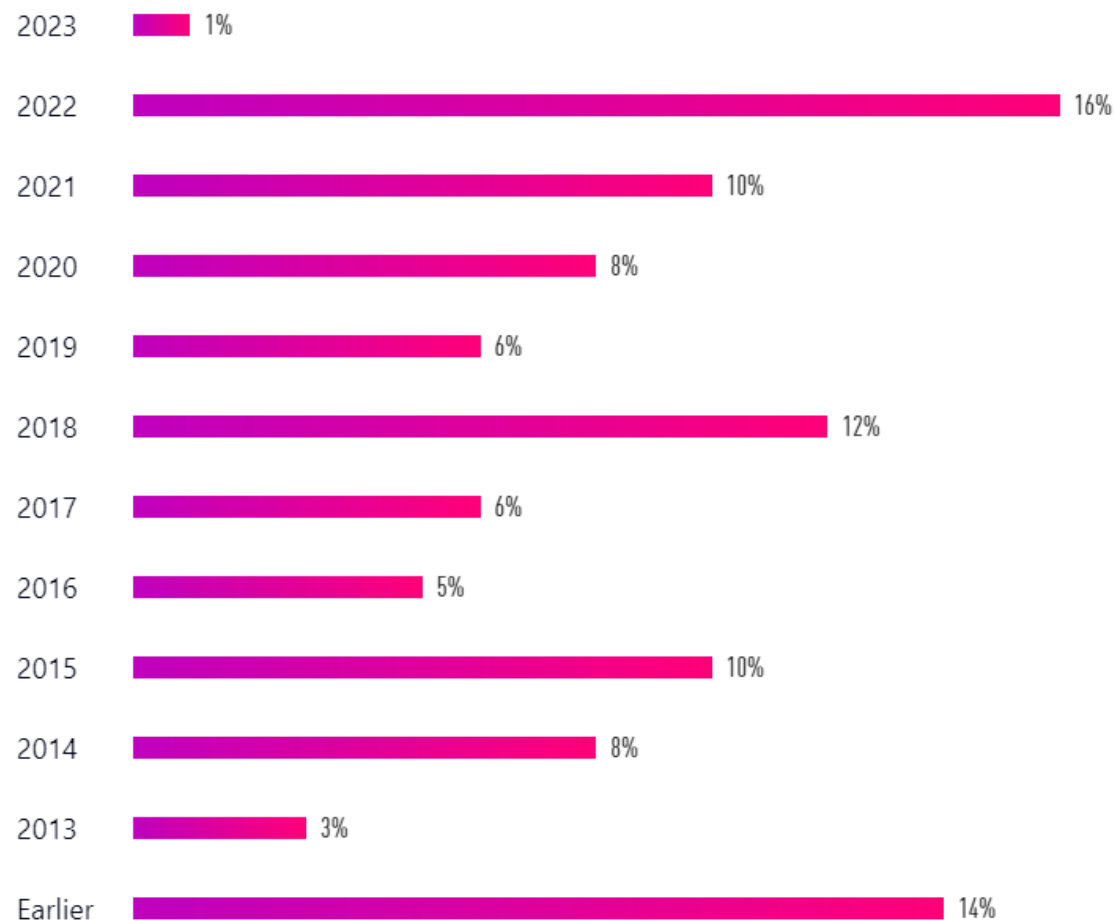


TOP MALWARE FAMILIES



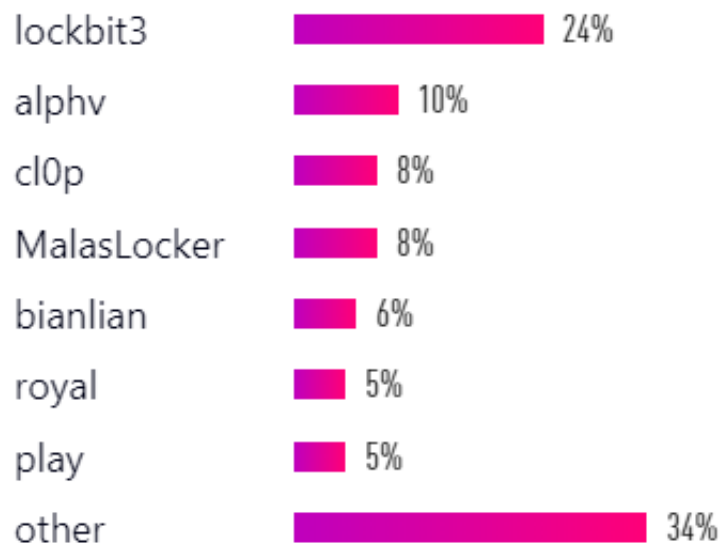
攻擊漏洞分析: 仍須著重於Patch管理與漏洞更新

PERCENTAGE OF ATTACKS LEVERAGING VULNERABILITIES BY DISCLOSURE YEAR IN H1 2023

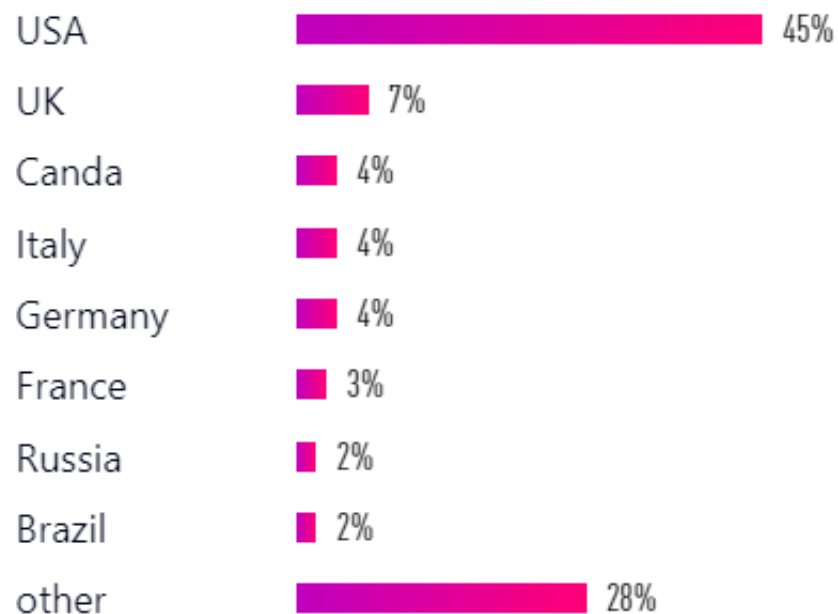


勒索軟體攻擊: 影響最鉅為製造、零售、軟體資訊

Most active actors by number of victims, as reported on shame sites - H1 2023.

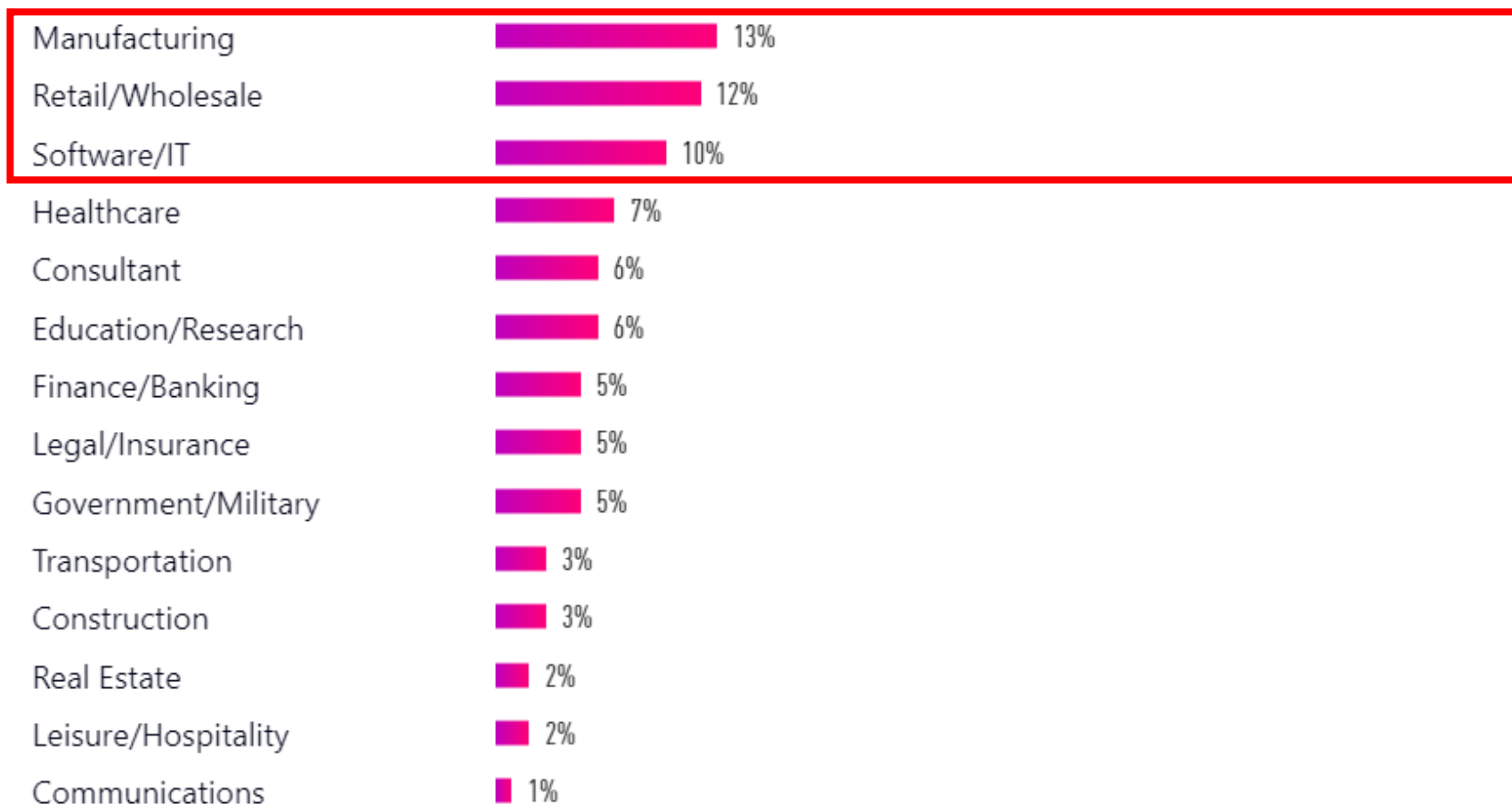


VICTIMS BY COUNTRY, AS REPORTED ON SHAME SITES - H1 2023.



勒索軟體攻擊: 影響最鉅為製造、零售、軟體資訊

INDUSTRY DISTRIBUTION OF RANSOMWARE VICTIMS, AS REPORTED ON SHAME SITES - H1 2023

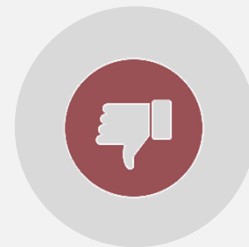


生成式AI- 對資安產業憂喜參半的創新科技應用



啟發更多創新網路防禦技術機會

- 更快速的系統開發整合
- 提升人員管理維運能力
- 增進事件分析準確度與回應效率



對日益增加的網路攻擊活動帶來隱憂

- 加速惡意程式變種與新型釣魚的生成
- 更巨量的偽冒身分資訊與內容
- 有效模擬測試攻擊以增加成功率



DD Will generative-AI accelerate cyber offense?

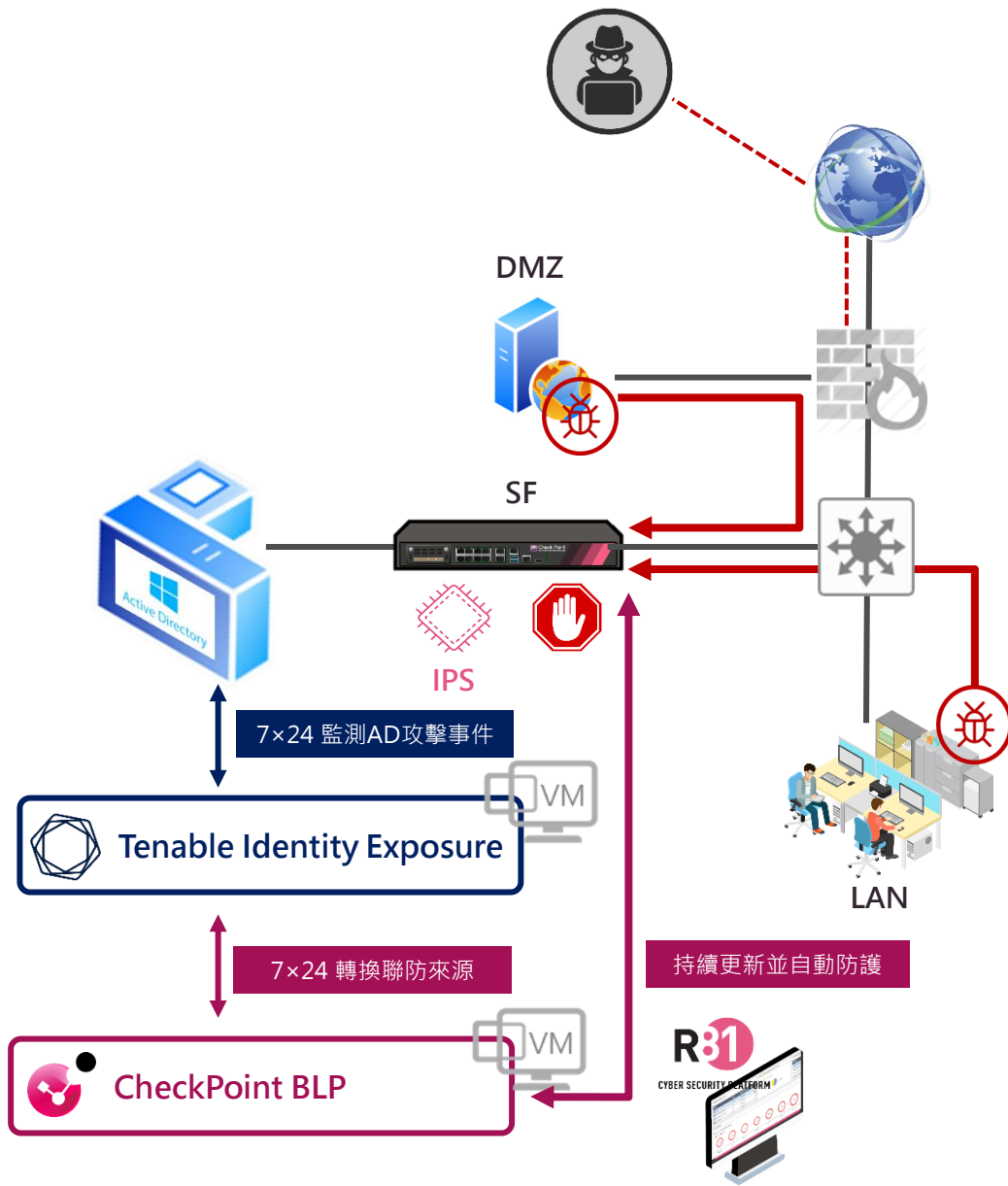


Yes, it is possible that generative-AI could be used to accelerate and automate various forms of cyber offenses, such as phishing attacks, malware generation, and misinformation campaigns. However, it is also possible that advancements in AI and machine learning could be used to enhance cybersecurity defenses and mitigate the potential impact of such attacks. The relationship between generative-AI and cybercrime is complex and dynamic, and will likely continue to evolve as technology advances.



我們正在處於歷史發展的轉折點!

聯防與即時緩解應用: 以AD關鍵設施為例



- **Tenable Identity Exposure (.ad)**
負責監控異常AD登入事件並將Syslog轉拋至CP BLP
- **CP BLP(Block List Parser/Birdlex Log Parser)**
蒐集由聯防來源(e.g. Tenable)的syslog資訊，建立事件觸發閾值(例如幾分鐘內發現幾次事件則提取IP至Web list)
也可整合其他CP產品如EDR/WAF等
- **Check Point Management**
建立動態物件(Network Feeds Object)與相關存取規則，後續可透過SmartConsole Extension調整CP BLP設定
- **Check Point Gateway**
負責抓取CP BLP內的Web List (Interval 最低一分鐘), 並透過規則進行阻擋(Deny)，Web List更新可設定阻擋時間(TTL)
- 加值整合應用
如通報MDR, 或以IFTTT整合Line通知等

建議: 運用AI智能情資與全域防護, 增進安全韌性



Call to Action: 申請數位資產安全韌性與健檢評估



Quantum



CloudGuard

全面網路資安可視性評估

內網流量與應用程式分析
網路APT解析與報表
Web服務與存取(WAF)



Harmony

雲端郵件與端點安全檢視
O365/SaaS郵件安全檢查(惡意程式與釣魚)
端點EDR分析與威脅獵捕



CloudGuard

雲端數位資產態勢風險感知

Cloud Posture安全管理
雲端安全事件與情資分析
風險感知與異常偵測



Horizon

XDR/XPR 資安監控與回應

全面性零時差盲點監控
情資整合與回應流程
AI智能威脅分析



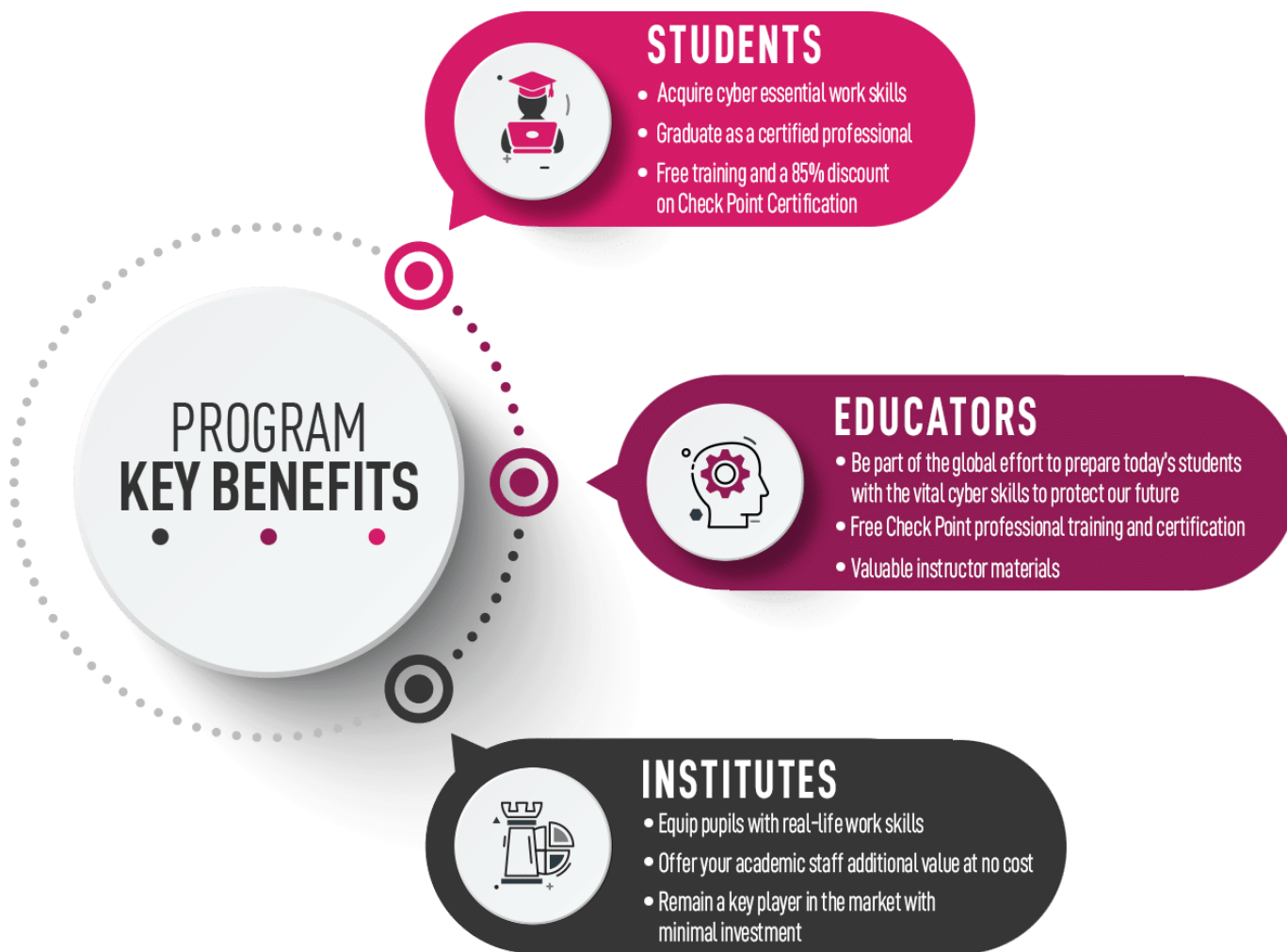


ONE MORE THING...

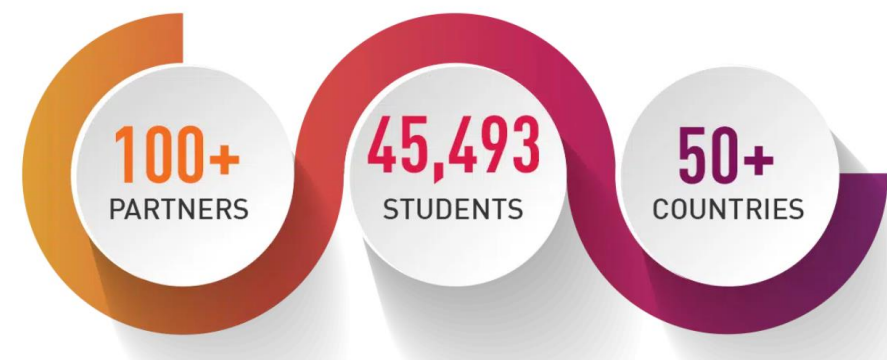
國際資安教育學苑計畫



產學合作計畫: 高教學府 x CP國際資安教育學苑



- * 符合在地化資安人才培育政策
- * 建立資安學習風氣
- * 專業技術與經驗交流
- * 配合高教深耕計畫(資安部分)
- * 參與新興研究計畫
- * 建立產學合作典範



國際資安教育學苑全球合作名校

期望與臺灣一流學府共同攜手合作
將全球最優異的資安資源落地臺灣



資安學苑線上學程入口 (可客製校名/Logo)

The screenshot displays the SecureAcademy eLearning interface. At the top, there is a header for 'SecureAcademy - Cyber Security Essentials | eLearning' with a 5-star rating and a 'Continue this learning path' button. Below this, there are three main course sections, each with a progress indicator of 0%:

- SecureAcademy - Digital Forensics Essentials | eLearning**
 - DFE course - EC-Council
 - 0% My Score
- SecureAcademy - Ethical Hacking Essentials | eLearning**
 - EHE course - EC-Council
 - 0% My Score
- SecureAcademy - Network Defense Essentials | eLearning**
 - NDE course - EC-Council
 - 0% My Score

Type 1:

業界資安通識課程

-EC-Council x Check Point

Type 2:

Check Point網路安全基礎課程

-產業技術與CP產品基礎訓練

Type 3:

資安密室逃脫-情境式解謎

採遊戲方式驗證學員能力

線上課程時數共約14-16小時

認證培育課程 (由合作學校種子受訓後自行開班)



CHECK POINT

CHECK POINT
CCSA
Certified Security Administrator
CERTIFICATION

CHECK POINT
CERTIFIED SECURITY ADMINISTRATOR
(CCSA)

AUDIENCE
Technical professionals who support, install, deploy or administer Check Point products.

GOALS
Learn basic concepts and develop skills necessary to administer IT security fundamental tasks.

PREREQUISITES
Working knowledge of Unix-like and Windows operating systems and TCP/IP Networking.



CHECK POINT

CHECK POINT
CCSE
Certified Security Expert
CERTIFICATION

CHECK POINT
CERTIFIED SECURITY EXPERT
(CCSE)

AUDIENCE
Technical Professionals who architect, upgrade, maintain, and support Check Point products.

GOALS
Learn advanced concepts and develop skills necessary to design, deploy, and upgrade Check Point Security environments.

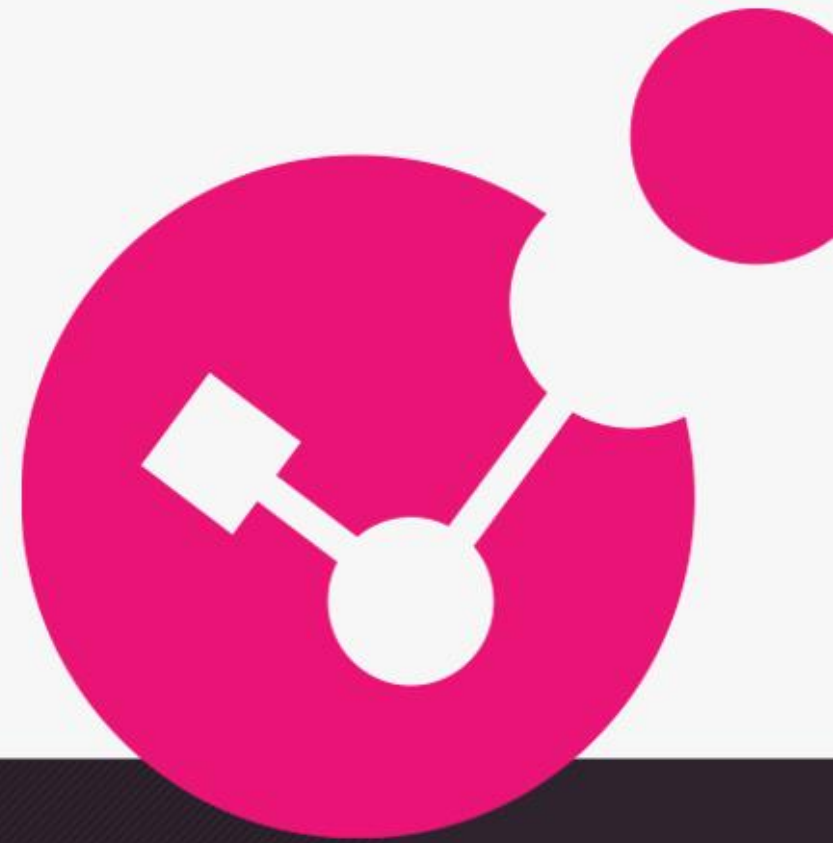
PREREQUISITES
CCSA Training or Certification, fundamental Unix and Windows knowledge, certificate management experience, system administration and networking knowledge.

含金量高的國際資安大廠證照
從事金融業、政府、大型企業資安人員認證
系統整合商、資安代理商技術工程師必備



Thank you!

Danny Yang, Cyber Security Evangelist
danny@checkpoint.com



YOU DESERVE THE BEST SECURITY